Notice of Allowability	Application No.	Applicant(s)	
	09/476,037	KORN R.	
	Examiner	Art Unit	
	Grigory Gurshman	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE filed 9/14/2004*.

2. ☒ The allowed claim(s) is/are *9,13-17 and 19-39*.

3. ☐ The drawings filed on _____ are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☒ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

THOMAS R. PEESO
PRIMARY EXAMINER

DETAILED ACTION

EXAMINER'S AMENDMENT

1. Applicant has substantially clarified the claimed invention in the course of the in person interview on 11/12/2004. Based on the discussion the application has been amended as follows:

Claim 9 : A method for preventing unauthorized alteration of content, comprising:

a) computing a hashed value for each executable command in a script;

b) encrypting the hashed value for each executable command in the script with a first ~~public encryption~~ private key of a first asymmetric key pair~~, wherein the first public encryption private key uses a first private key to encrypt the hashed value for each executable command;~~

c) appending to the script the encrypted hashed values for each executable command;

d) ~~providing~~ embedding a first public key corresponding to the first private key to an interface control, comprising a script; and

e) signing the interface control , wherein signing the interface control comprises encrypting the interface control using a second ~~public encryption~~ private key of a second asymmetric key pair, ~~wherein the second public encryption private key uses a second public key,~~ the signature for the interface control for hiding the first public key provided therein, wherein the signed interface control is used to invoke the script.

Claim 16 : A method for secure execution of content, comprising:

a) verifying a ~~public key cryptography~~ signature associated with an interface control using a second public key from a second asymmetric key pair, the interface control comprising a script;

b) computing a hashed value for each executable command in the script;

c) decrypting an encrypted hashed value appended to the script for each executable command in the script using a first public key from a first asymmetric key pair to obtain a decrypted hashed value for each executable command in the script;

d) comparing the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script; and

e) executing the executable commands in the script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands.

Claim 23: An article of manufacture comprising a machine accessible medium providing a plurality of machine readable instructions, wherein the instructions, when executed by a processor, cause the processor to:

a) compute a hashed value for each executable command in a script;

b) encrypt the hashed value for each executable command in the script with a first ~~public encryption~~ private key of a first asymmetric key pair~~, wherein the first public~~

~~encryption private key uses a first private key to encrypt the hashed value for each executable command to the script;~~

c) append to the script the encrypted hashed values for each executable command;

d) ~~provide~~ embed a first public key corresponding to the first private key to an interface control comprising a script; and

e) sign the interface control, wherein instructions to sign the interface control comprise instructions to encrypt the interface control using a second ~~public encryption~~ private key of a second asymmetric key pair, ~~wherein the second public encryption private key uses a second public key,~~ the signature for the interface control for hiding the first public key provided therein, wherein the signed interface control is used to invoke the script.

Claim 24: An article of manufacture comprising a machine accessible medium providing a plurality of machine readable instructions, wherein the instructions, when executed by a processor, cause the processor to:

a) verify a ~~public key cryptography~~ signature associated with an interface control using a second public key from a second asymmetric key pair ~~comprising a script~~ in response to activating the interface control, the interface control comprising a script;

b) compute a hashed value for each executable command in the script;

c) decrypt an encrypted hashed value appended to the script for each executable command in the script using a first public key from a first asymmetric key pair to obtain a decrypted hashed value for each executable command in the script;

d) compare the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script; and

e) execute the executable commands in the script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands.

Claim 25 : An apparatus, comprising:

a server computer, the server computer including a database to house and serve web pages and a server processor to:

compute a hashed value for each executable command in a script on a web page;

encrypt the hashed value for each executable command in the script with a first ~~public encryption~~ private key of a first asymmetric key pair~~, wherein the first public encryption private key utilizes a first private key to encrypt the hashed value for each executable command in the script;~~

append to the script the encrypted hashed values for each executable command;

~~provide~~ embed a first public key corresponding to the first private key to an interface control comprising a script; and

sign the interface control, wherein to sign the interface control includes to encrypt the interface control using a second ~~public encryption~~ private key of a second asymmetric key pair, ~~wherein the second public encryption private key uses a second public key,~~ the signature for the interface control for hiding the first public key provided therein, wherein the signed interface control is used to invoke the script.

Claim 38: The method of claim 16, wherein prior to verifying a ~~public key cryptography~~ signature associated with an interface control comprising a script, downloading a web page to enable a user to activate the interface control, wherein the interface control is contained in the web page.

Claim 39 : The method of claim 16, wherein verifying a ~~public key cryptography~~ signature associated with an interface control comprising a script comprises:

decrypting the ~~public key cryptography~~ signature associated with the interface control using ~~a~~ the second public key, wherein the ~~public key cryptography~~ signature hides a first public key;

determining whether changes have occurred to either the interface control or the ~~public key cryptography~~ signature associated with the interface control; and

detecting the changes, if the changes have occurred.

Allowable Subject Matter

2. Claims 9, 13 - 17, 19 - 39 are allowed.

3. The following is an examiner's statement of reasons for allowance:

3.a Referring to the independent claims 9, 16, 23, 24, 25 and 27, Atkinson disclosed a method for creating a secure script (see abstract). Atkinson teaches that the method comprises:

computing a hashed value for at least one executable command in the script; (see FIG. 3 - a flow diagram representing a code certification or signing method for ensuring the authenticity and integrity of a computer program, code, or an executable file received over computer network, or any other computer network – col. 6, line 19-23). Atkinson shows a process block indicating that a cryptographic digest or "hash" (FIG. 4) of executable file is obtained or computed (col. 6, line 39-41). Atkinson, however, does not teach *computing a hashed value for each executable command in the script.* Atkinson also does not teach the script being an *interface control script*.

Referring to the instant claims, Atkinson shows that a process block indicates that a publisher signature (FIG. 4) is formed with cryptographic digest. (col 6, line 50-51). The public key is used (see Fig.3). Signing the control program, comprising the public key is shown in Fig.4. The instant claims, however, recite *encrypting the hashed value for each executable command in the script with a private key*. Therefore Atkinson teaches a different way of using an asymmetric key encryption schema.

Atkinson teaches that the publisher signature is attached or appended to or incorporated to executable file (the last line of col. 6 continue to the first line of col. 7).

However, Atkinson does not teach appending the script to each executable command within the control.

Atkinson does not teach or suggest *embedding a first public key to the interface control comprising a script.* Atkinson also does not teach or suggest using two levels of encryption, wherein signing the *interface control comprises encrypting the interface control using the second private key of a second asymmetric pair.*

Referring to claims 25 and 27, Atkinson does not teach signing the interface control with a second private key in order to hide the first public key embedded into the control script.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Drawings

4. The drawings filed on 12/31/1999 are acceptable subject to replacement of all figures drawn by hand. In order to avoid abandonment of this application, correction is required in reply to the Office action. The correction will not be held in abeyance.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (571)272-3803. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Grigory Gurshman
Examiner
Art Unit 2132

GG

THOMAS R. PEESO
PRIMARY EXAMINER